

Ochrona i bezpieczeństwo danych pomiarowych w kontekście projektu nowego Prawa energetycznego oraz ostatniej nowelizacji aktualnego Prawa energetycznego

Spis treści

- I. Wstęp
- II. Ochrona i bezpieczeństwo danych pomiarowych na gruncie prawa europejskiego
- III. Ochrona i bezpieczeństwo danych pomiarowych na gruncie prawa polskiego. Ewolucja dotychczasowych propozycji legislacyjnych i obecny stan prawny
 1. „Duży trójpak”
 2. „Mały trójpak”
- IV. Ocena ostatniej nowelizacji Prawa energetycznego w zakresie ochrony i bezpieczeństwa danych pomiarowych
 1. Brak obowiązku instalacji inteligentnych liczników
 2. Obowiązek ochrony danych pomiarowych zgodnie z przepisami ustawy o ochronie danych osobowych
- V. Potrzeba nowelizacji polskich przepisów prawa w zakresie ochrony i bezpieczeństwa danych pomiarowych
 1. Czy przepisy ustawy o ochronie danych osobowych są wystarczające?
 2. Spodziewane zmiany w systemie ochrony danych osobowych na poziomie unijnym
 3. Potrzeba zmian w polskim prawie
- VI. Zakończenie

Streszczenie

Autor poddaje analizie potrzebę kompleksowego uregulowania w polskim systemie prawnym zagadnień ochrony i bezpieczeństwa danych pomiarowych pozyskiwanych za pomocą inteligentnych liczników. Analizuje on w tym zakresie przepisy i wytyczne unijne oraz obowiązujące przepisy polskie, w tym ostatnią nowelizację aktualnego Prawa energetycznego¹, a także projekt nowego Prawa energetycznego. W konsekwencji wskazuje na potrzebę kompleksowej regulacji ochrony i bezpieczeństwa danych pomiarowych w polskich przepisach, realizującej zalecenia unijne w tym zakresie.

Słowa kluczowe: dane pomiarowe; dane osobowe; inteligentne liczniki; inteligentne sieci; ochrona danych pomiarowych; bezpieczeństwo danych pomiarowych.

* Radca prawny w kancelarii WBK Wierciński Kwieciński Baehr. Absolwent Wydziału Prawa Uniwersytetu im. Adama Mickiewicza w Poznaniu oraz Wydziału Prawa Uniwersytetu Europejskiego Viadrina we Frankfurcie nad Odrą, gdzie uzyskał tytuł Master of German and Polish Law (LLM).

¹ Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz.U. z 2012 r. Nr 1059 z późn zm.); dalej: PE.

I. Wstęp

Od ponad dwóch lat toczy się dyskusja na temat potencjalnego wdrożenia w Polsce systemu inteligentnego opomiarowania w kontekście odbiorców końcowych², czyli systemu pomiaru i kontroli zużycia energii elektrycznej przy wykorzystaniu tzw. inteligentnego licznika (ang. *smart meter*)³. Celowo użyto słowa potencjalnego, ponieważ wbrew pozorom ostateczna decyzja w tej kwestii nie została jeszcze podjęta, pomimo wymogów dyrektywy 2009/72/WE oraz grożącej Polsce kary za brak jej pełnej implementacji⁴. Niemniej mogło wydawać się inaczej, biorąc pod uwagę projekt zupełnie nowego prawa energetycznego (dalej: nowe PE) zgłoszony w ramach tzw. dużego trójpacku⁵, przewidujący powszechne wdrożenie w Polsce systemu inteligentnego opomiarowania odbiorców końcowych w ściśle określonym czasie. W konsekwencji projekt ten zawierał także szereg przepisów poświęconych zbieraniu, przetwarzaniu i udostępnianiu danych pomiarowych⁶, przy czym gros tych przepisów miało na celu zapewnienie odpowiedniego poziomu bezpieczeństwa i ochrony tych danych. Jednocześnie dyskusje fachowców co do przyszłego modelu wdrożenia systemu inteligentnego opomiarowania również dotyczyły głównie aspektów ochrony i bezpieczeństwa danych pomiarowych. Wydaje się to zrozumiałe. Oprócz wielu zalet, jakie niewątpliwie może przynieść powszechne wdrożenie inteligentnego opomiarowania, dostrzega się również wady tego rozwiązania, a co za tym idzie – największe zagrożenie, czyli potencjalną ingerencję w prywatność odbiorców energii. Prawo do prywatności jest z kolei jednym z podstawowych praw obywatelskich zapisanych w Karcie praw podstawowych Unii Europejskiej⁷ oraz w Traktacie o Funkcjonowaniu Unii Europejskiej (dalej: TFUE)⁸. Właśnie dlatego, że mowa jest o potencjalnym zagrożeniu dla jednego z podstawowych praw, ochrona danych pomiarowych budzi tyle emocji. Jak ważny jest to aspekt pokazują także zagraniczne przykłady, gdzie spowodowany obawą przed naruszeniem prywatności społeczny opór skutecznie ograniczył powszechne wdrożenie systemu inteligentnego opomiarowania⁹. Mając powyższe na uwadze, można zaryzykować

² W szerszym kontekście system inteligentnego opomiarowania obejmuje także inteligentne sterowanie sieciami elektroenergetycznymi oraz przyłączonymi do nich źródłami wytwórczymi.

³ Inteligentny licznik to licznik zapamiętujący zużycie danego odbiorcy i komunikujący to zużycie dystrybutorowi i sprzedawcy energii elektrycznej dla celów monitoringowych i bilingowych. Dzięki tym informacjom, odbiorcy są w stanie bezpośrednio kontrolować i zarządzać swoim zużyciem, a dystrybutorzy lepiej planować obciążenie systemu i jego bilansowanie, np. w kontekście integracji sieci z odnawialnymi źródłami energii. Zob. Q&A on the deployment of smart electricity grids and smart meters. Memo KE z 12 kwietnia 2011 r. Pobrano z: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/20110412_memo.pdf.

⁴ W tym kontekście trzeba wskazać, iż zgodnie z dyrektywą 2009/72/WE, na Polsce ciąży obowiązek instalacji inteligentnych systemów pomiarowych u przynajmniej u 80% odbiorców do 2020 r. (zob. Załącznik I pkt 2 te same dyrektywy), ponieważ Polska nie przeprowadziła przewidzianej w dyrektywie ekonomicznej oceny wszystkich długoterminowych kosztów i korzyści dla rynku oraz indywidualnego konsumenta wdrożenia systemu inteligentnego opomiarowania, której ewentualny negatywny wynik pozwoliłby na niewdrożenie tego systemu w Polsce. Powszechnie uważa się, że jeżeli dany kraj nie przeprowadził takiej oceny, to obowiązek montażu inteligentnych systemów pomiarowych u 80% odbiorców do 2020 r. jest bezwarunkowy; zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Inteligentne sieci: od innowacji do wdrożenia (KOM(2011) 202, s. 3).

⁵ Pakiet projektów nowych ustaw regulujących kwestie zawarte dotychczas w PE, w skład którego wchodzi projekt nowego prawa energetycznego, nowego prawa gazowego, nowej ustawy o odnawialnych źródłach energii oraz przepisów wprowadzających ustawę – Prawo energetyczne, ustawę – Prawo gazowe oraz ustawę o odnawialnych źródłach energii. Projekty w aktualnych wersjach dostępne są na stronach RCL.

⁶ Przez dane pomiarowe rozumiem dane o zużyciu energii zbierane i przekazywane przez inteligentny licznik.

⁷ Zgodnie z art. 7 Karty Praw Podstawowych UE każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. Ponadto zgodnie z art. 8 Karty każdy ma prawo do ochrony danych osobowych, które go dotyczą. Ujęcie prawa do prywatności w Karcie podkreśla jego rangę. Zakres obowiązywania Karty w Polsce pozostaje natomiast bez praktycznego znaczenia, biorąc pod uwagę, iż prawo do prywatności gwarantowane jest także na poziomie traktatów unijnych.

⁸ Zgodnie z art. 16 ust. 1 TFUE każdy ma prawo ochrony danych osobowych, które go dotyczą.

⁹ Przykładowo w Stanach Zjednoczonych, w odpowiedzi na powszechne w wielu stanach inicjatywy montażu inteligentnych liczników podejmowane przez operatorów, powstało szereg organizacji społecznych sprzeciwiających się tego typu projektom, wskazując głównie na zagrożenie prywatności (np. stopsmartmeters.org, stopsmartmetersnow.com). W konsekwencji organizacje te na szeroką skalę prowadziły i prowadzą akcję *opt out*, zachęcając ludzi do niewyrażania zgody na montaż inteligentnych liczników lub do żądania ich demontażu i ponownego montażu klasycznego licznika. Wskutek takich akcji w wielu przypadkach przyjęto model *opt out* dający odbiorcom możliwość niewyrażenia zgody na montaż inteligentnego licznika; np. w Kalifornii, firma Pacific Gas & Electric, która zainstalowała 8,7 miliona inteligentnych liczników, na skutek oporu społecznego została zmuszona przez Public Utilities Commission do zagwarantowania odbiorcom prawa *opt out*. Pobrano z: <http://www.midwestenergynews.com/2012/01/24/as-smart-meters-roll-out-opponents-get-organized/>.

stwierdzenie, że ochrona i bezpieczeństwo danych pomiarowych są najważniejszym czynnikiem ograniczającym swobodę pozyskiwania, przetwarzania i udostępniania danych pomiarowych. W konsekwencji aspekt ochrony i bezpieczeństwa danych pomiarowych będzie miał kluczowe znaczenie dla przyjętego w Polsce modelu inteligentnego opomiarowania. Bez zapewnienia odpowiedniego poziomu ochrony na poziomie ustawowym, argumenty przeciwników inteligentnego opomiarowania mogą skutecznie dotrzeć do odbiorców, którzy w obawie przed potencjalnym zagrożeniem prywatności mogą sprzeciwiać się montażowi inteligentnych liczników. Tego rodzaju powszechny sprzeciw może z kolei przekreślić szanse na osiągnięcie zamierzonych celów wdrożenia inteligentnego opomiarowania, jakim jest przede wszystkim zmniejszenie zużycia energii w skali makro¹⁰. Jednocześnie jak wskazano na wstępie, koncepcja wdrożenia systemu inteligentnego opomiarowania, a w konsekwencji ochrony danych pomiarowych w polskim systemie prawnym nie została jeszcze przesądzona¹¹. Ponieważ ostatnia nowelizacja PE w zakresie ochrony danych pomiarowych była niezwykle lapidarna, a jednocześnie prace nad nowym PE zgodnie z deklaracjami rządu mają być kontynuowane, warto rozważyć czy aktualna regulacja w zakresie ochrony i bezpieczeństwa danych pomiarowych jest wystarczająca i ewentualnie, w jaki sposób kwestie te powinny zostać uregulowane w nowym PE.

II. Ochrona i bezpieczeństwo danych pomiarowych na gruncie prawa europejskiego

Aby odpowiedzieć na pytanie, czy polskie przepisy w zakresie ochrony i bezpieczeństwa danych pomiarowych są wystarczające, należy w pierwszej kolejności przyjrzeć się unijnym regulacjom i wytycznym w tym zakresie.

Powszechnie przyjmuje się, że dane pomiarowe mogą stanowić dane osobowe, ponieważ choćby pośrednio pozwalają na odtworzenie profilu zażycia energii indywidualnego odbiorcy¹². Konsekwencją powyższego jest stosowanie do danych pomiarowych unijnych dyrektyw dotyczących ochrony danych osobowych, tj. dyrektywy 95/46/WE oraz dyrektywy 2002/58/WE¹³. Dyrektywy te zawierają szereg ogólnych zasad ochrony i bezpieczeństwa wszelkich danych

Warto przy tym wskazać, że niektóre przedsiębiorstwa energetyczne podjęły działania w kierunku umożliwienia pobierania opłat od odbiorców korzystających z *opt out*. Przedsiębiorstwa energetyczne argumentują m.in., że brak inteligentnego licznika powoduje wzrost kosztów obsługi odbiorcy, konieczne jest bowiem osobiste dokonywanie odczytów. Sytuacja taka ma miejsce np. w stanie Maryland. Pobrano z: http://articles.baltimoresun.com/2013-08-05/business/bs-bz-smart-meter-opt-out-cost-20130805_1_digital-meters-radio-frequency-emissions-maryland-electric-cooperative.

¹⁰ W skali mikro montaż inteligentnego licznika pozwoli na obniżenie zużycia energii poszczególnemu odbiorcy. W skali makro natomiast inteligentne liczniki należy postrzegać jako element sieci elektroenergetycznych pozwalający na optymalizację ich pracy (a w tym m.in. obniżenie strat i lepsze planowanie produkcji) dzięki sygnałom o zużyciu wysyłanym przez te liczniki. Zob. F.M. Elżanowski, M.M. Sokolowski, *Smart grids i smart metering w procesie inwestycyjnym*, [w:] M. Cherka, F.M. Elżanowski, MK. Swora, K.A. Wąsowski (red.), *Energetyka i ochrona środowiska w procesie inwestycyjnym*, Oficyna Wolters Kluwer Polska, Warszawa 2010, pkt 3. Aby jednak osiągnąć powyższy cel w skali makro, montaż liczników inteligentnych musi być powszechny.

¹¹ Potwierdza to ewolucja proponowanych dotychczas regulacji w tym zakresie, od początkowych, relatywnie rozbudowanych rozwiązań w „dużym trójpaku”, poprzez nieco okrojone propozycje w pierwszych projektach „małego trójpaku”, aż po niemalże zdawkowe rozwiązania przyjęte w ostatniej nowelizacji PE.

¹² Odczytanie danych pomiarowych z konkretnego licznika inteligentnego nie daje oczywiście jeszcze możliwości ustalenia z całą pewnością zindywidualizowanego odbiorcy energii. Niemniej już choćby tylko sięgając do umowy sprzedaży energii, można z dużym prawdopodobieństwem zidentyfikować danego odbiorcę. Nawet, jeżeli w danym gospodarstwie domowym będzie więcej odbiorców energii elektrycznej (niż strona umowy) albo stroną umowy sprzedaży będzie osoba w ogóle niezamieszkująca danego gospodarstwa domowego (np. w przypadku wynajmu mieszkania), to i tak w dalszym ciągu przy użyciu odpowiednich środków można ustalić faktycznych odbiorców energii. W powyższym kontekście trzeba wskazać, że zgodnie z definicją zawartą w dyrektywie 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, dane osobowe oznaczają wszelkie informacje dotyczące nie tylko konkretnej osoby, lecz także osoby możliwej do zidentyfikowania i to choćby w pośredni sposób. Definicję tę przy tym należy wyklądać szeroko. W konsekwencji upowszechnił się pogląd, iż dane pomiarowe mogą stanowić dane osobowe; zob. R. Knyrim, G. Trieb, *Smart metering under EU data protection law*, „International Data Privacy Law” 2011, Vol. 1, s. 123). W konsekwencji w dalszej części artykułu wymogi i wytyczne dotyczące danych osobowych odniesiono bezpośrednio do danych pomiarowych.

¹³ Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej). Dyrektywa o prywatności i łączności elektronicznej znajduje zastosowanie ze względu na zdalne przesyłanie danych pomiarowych z liczników inteligentnych do miejsca ich gromadzenia za pośrednictwem łącza elektronicznego.

osobowych bez względu na ich rodzaj. W konsekwencji zasady te pozostają aktualne także w odniesieniu do danych pomiarowych. Pośród najważniejszych z nich należy wskazać zasadę jak najmniejszego ingerowania, zakładającą obowiązek minimalizacji zakresu przetwarzanych danych z punktu widzenia celu, dla którego dane te są przetwarzane. Z kolei zgodnie z zasadą przejrzystości, należy informować w przyjazny, klarowny i prosty sposób o celach, terminach i okolicznościach gromadzenia, przechowywania oraz o wszystkich dalszych działaniach w zakresie przetwarzania danych. Ponadto archiwizowanie danych pomiarowych powinno być dozwolone tylko w jasno określonym, klarownym celu. Z dyrektyw unijnych wynika także wymóg uzyskania świadomej i dobrowolnej zgody na każdy rodzaj przetwarzania danych z możliwością cofnięcia zgody w każdym momencie bez konsekwencji¹⁴, oraz wymóg określenia zasad wglądu odbiorców w swoje dane pomiarowe i zapewnienia możliwości wprowadzania w nich zmian, w tym ich usunięcia¹⁵. Wreszcie należy wskazać zasadę stosowania najlepszych dostępnych technik w celu zapewnienia bezpieczeństwa przechowywanych danych pomiarowych, oznaczającą konieczność stosowania najlepszych dostępnych rozwiązań technicznych w celu uniknięcia nieuprawnionego pozyskania lub zmodyfikowania danych. Obie dyrektywy zostały implementowane do prawa polskiego. Powyższe zasady obowiązują już zatem w polskim porządku prawnym i należy je stosować także do danych pomiarowych¹⁶. Z punktu widzenia konieczności wprowadzenia ewentualnych zmian w polskich przepisach prawa, wytyczne wynikające z tych dyrektyw pozostają zatem bez praktycznej doniosłości.

Niemniej obok wyżej wskazanych dyrektyw, pewien standard w zakresie ochrony i bezpieczeństwa stricte danych pomiarowych wyznaczają także inne unijne dokumenty o charakterze *soft law*, zawierające niewiążące wytyczne skierowane do państw członkowskich. Za najważniejsze tego typu dokumenty, wyznaczające pewien pożądaný w UE standard ochrony i bezpieczeństwa danych pomiarowych, należy uznać Zalecenia KE, rekomendacje¹⁷ Grupy Zadaniowej ds. Inteligentnych Sieci, Grupy Ekspertów 2¹⁸ oraz opinię¹⁹ Grupy Roboczej ds. Ochrony Danych²⁰. Szczegółowe omówienie wszystkich tych wytycznych przekracza ramy niniejszego artykułu. Niemniej można z nich wyprowadzić pewne wspólne, najważniejsze zalecenia w zakresie ochrony i bezpieczeństwa danych pomiarowych. Po pierwsze zaleca się, aby ochrona danych pomiarowych była brana pod uwagę już w fazie projektowania systemu opomiarowania²¹. Ponadto kierując się zasadą poufności danych z założenia, liczniki inteligentne powinny być domyślnie ustawione na ochronę

¹⁴ W odniesieniu do danych pomiarowych, jak się wydaje, zasada ta powinna znaleźć zastosowanie w ograniczonym zakresie, a mianowicie cofnięcie zgody odbiorcy powinno odnosić skutek wyłącznie na przyszłość. Mając na uwadze charakter danych pomiarowych i cel ich gromadzenia, nieracjonalne byłoby bowiem umożliwienie odbiorcy cofnięcia zgody ze skutkiem wstecznym, co mogłoby np. uniemożliwić dokonanie rozliczeń. Powyższe stanowisko, jak się wydaje, podziela także KE, stwierdzając, iż „odwołanie zgody nie powinno mieć wpływu na zgodność z prawem przetwarzania opartego na zgodzie przed jej odwołaniem”. Zob. Zalecenia Komisji 2012/148/WE z dnia 9 marca 2012 r. w sprawie przygotowań do rozpowszechnienia inteligentnych systemów opomiarowania, pkt I, ust. 20 (dalej: Zalecenia KE).

¹⁵ Uprawnienie to jednak, jak się wydaje, nie powinno dawać odbiorcy możliwości do zmiany danych wynikających z dokonanych pomiarów.

¹⁶ Jak wskazywałem wyżej, dane pomiarowe można traktować jak dane osobowe i z tego względu do danych pomiarowych mają zastosowanie zasady ochrony i bezpieczeństwa danych osobowych.

¹⁷ Regulatory Recommendations for Data Safety, Data Handling and Data Protection [Zalecenia regulacyjne w zakresie bezpieczeństwa, przetwarzania i ochrony danych], Raport z 16 lutego 2011 r. Pobrano z: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

¹⁸ Dyrekcja Generalna ds. Energii KE powołała do życia Grupę Zadaniową ds. Inteligentnych Sieci, Grupę Ekspertów 2, stanowiącą część Grupy Zadaniowej, w celu ułatwienia i wsparcia procesu wdrażania inteligentnych sieci w UE.

¹⁹ Opinia 12/2011 przyjęta 4 kwietnia 2011 r. na temat inteligentnego pomiaru zużycia; Grupa Zadaniowa ds. Inteligentnych Sieci, Grupa Ekspertów 2.

²⁰ Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest niezależnym europejskim organem doradczym w zakresie ochrony danych osobowych i prywatności.

²¹ Zgodnie z pkt I ust. 3 Zaleceń KE „ochrona danych w fazie projektowania” wymaga wdrożenia, z uwzględnieniem najnowszych osiągnięć technicznych oraz kosztów wdrożenia zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, odpowiednich środków i procedur technicznych i organizacyjnych, tak aby przetwarzanie odpowiadało wymogom dyrektywy 95/46/WE oraz gwarantowało ochronę praw osoby, której dotyczą dane.

danych²². Krajowe przepisy prawa powinny ponadto z góry określać dozwolone cele gromadzenia i udostępniania danych pomiarowych przy zachowaniu wymogu odrębnej zgody odbiorcy dla każdego celu. Co więcej, zaleca się określenie maksymalnych okresów archiwizowania danych pomiarowych, po upływie których powinny być one usunięte (okresy te mogą być uzależnione od różnych celów) oraz ustanowienie obowiązku usunięcia danych po cofnięciu przez odbiorcę zgody na ich przetwarzanie. W aspekcie technicznym, zaleca się stosowanie kodowanych kanałów przekazu, uniemożliwiających przechwycenie lub zmanipulowanie danych w trakcie ich przesyłania i utrudniających ataki hakerskie. Rekomenduje się także określenie obowiązków w zakresie bezpieczeństwa i ochrony danych pomiarowych w odniesieniu do wszystkich podmiotów, którym są one udostępniane, a ponadto zaleca się, aby podmioty te weryfikować w celu sprawdzenia, czy są odpowiednimi i kompetentnymi odbiorcami danych (podmioty te powinny zaś mieć dostęp do danych pomiarowych wyłącznie w zakresie koniecznym do realizacji ich funkcji). Wreszcie zaleca się określenie systemu oceny skutków w zakresie ochrony danych pomiarowych. Ponadto Grupa Robocza ds. Ochrony Danych w swojej opinii postuluje także utworzenie centrum informacyjno-komunikacyjnego, za pośrednictwem którego wszystkie zaangażowane strony uzyskiwałyby dostęp do danych konsumentów oraz stworzenie kodeksu, który wszystkie strony miałyby obowiązek podpisać oraz karty obowiązującej całą branżę.

W przypadku braku szczególnych unijnych aktów prawnych odnoszących się do danych pomiarowych, jak się wydaje, to właśnie wskazane wyżej miękkie wytyczne, zawierające bardziej szczegółowe zalecenia odnoszące się do danych pomiarowych, powinny stanowić punkt odniesienia przy ocenie czy polskie przepisy prawa i ostatnie propozycje ich zmian są wystarczające do zapewnienia odpowiedniej ochrony i bezpieczeństwa danych pomiarowych. W praktyce bowiem wytyczne te są skierowane właśnie do państw członkowskich, które powinny brać je pod uwagę przy tworzeniu prawa krajowego (choć oczywiście nie są do tego zobowiązane).

III. Ochrona i bezpieczeństwo danych pomiarowych na gruncie prawa polskiego. Ewolucja dotychczasowych propozycji legislacyjnych i obecny stan prawny

1. „Duży trójpak”

Pierwszą propozycję uregulowania kwestii związanych z montażem inteligentnych liczników oraz zbieraniem, przechowywaniem i udostępnianiem danych pomiarowych zawierał projekt nowego PE. Ostatnia upubliczniona wersja tego projektu z 8 października 2012 r. zawierała relatywnie kompleksową regulację dotyczącą wdrożenia w Polsce systemu inteligentnego opomiarowania²³. Po pierwsze, projekt nowego PE przewiduje obowiązek montażu liczników inteligentnych przez operatorów systemów dystrybucyjnych u ich odbiorców do 31 grudnia 2020 r. Po drugie, projekt przewiduje powołanie niezależnego operatora informacji pomiarowych (dalej: OIP), odpowiedzialnego za gromadzenie, przetwarzanie i udostępnianie podmiotom trzecim danych pomiarowych, przy czym zgodnie z projektem OIP powinien wykonywać swoje obowiązki, uwzględniając

²² Jak się wskazuje w opinii Grupy Roboczej ds. Ochrony Danych (s. 10), „na najbardziej podstawowym poziomie koncepcja „prywatności z założenia” zapewnia przesyłanie odczytów licznika wyłącznie z taką częstotliwością, jaka jest konieczna dla funkcjonowania systemu lub świadczenia usługi, na jaką zgodził się klient”.

²³ Projekt dostępny na stronach RCL pod adresem: <http://legislacja.rcl.gov.pl/lista/2/projekt/19295/katalog/68650>.

wymagania w zakresie bezpieczeństwa użytkowników systemu elektroenergetycznego, ochrony i poufności ich danych. Co więcej, projekt zakłada obowiązek opracowania przez OIP instrukcji informacji pomiarowych, określającej m.in. wymagania w zakresie bezpieczeństwa informacji pomiarowych, w celu ochrony odbiorców i użytkowników systemu, do której powinni stosować się wszyscy użytkownicy systemu elektroenergetycznego. Ponadto, na OIP nałożono obowiązek usunięcia danych pomiarowych w przypadku braku uzasadnienia dalszego ich archiwizowania, a także obowiązek sporządzenia raz na 2 lata, na okres 3 lat, programu przedsięwzięć, jakie należy podjąć w celu zapewnienia bezpieczeństwa i poufności informacji pomiarowych, zawierający harmonogram przedsięwzięć inwestycyjnych mających na celu utrzymanie standardów niezawodności świadczonych usług, z uwzględnieniem wymaganego poziomu bezpieczeństwa informacji oraz postępu technologicznego, podlegający zatwierdzeniu przez Prezesa Urzędu Regulacji Energetyki. Wyraźnie widać, że w projekcie nowego PE wielokrotnie podkreślono aspekt bezpieczeństwa i poufności danych w kontekście działań OIP. Można wręcz zaryzykować stwierdzenie, że wymóg bezpieczeństwa i poufności danych pomiarowych podniesiono do rangi głównej zasady, którą w swych działaniach powinien kierować się OIP. Co więcej, projekt nowego PE przewidywał także pewne ograniczenia swobody udostępniania danych pomiarowych. I tak już w samej ustawie przewidziano katalog podmiotów, którym OIP będzie mógł udostępniać dane pomiarowe. Ponadto wprowadzono zakaz dalszego udostępniania jednostkowych danych pomiarowych danego odbiorcy²⁴ (niezagregowanych), a udostępnianie danych w celu przygotowania oferty zgodnie z projektem ma być dopuszczalne wyłącznie sprzedawcy upoważnionemu przez odbiorcę końcowego. Bardziej szczegółowe kwestie w zakresie bezpieczeństwa i poufności danych pomiarowych zgodnie z projektem nowego PE mają być uregulowane w rozporządzeniu wykonawczym, a ponadto także w instrukcji informacji pomiarowych przygotowanej przez OIP.

Porównując przytoczone wcześniej wymogi, wynikające z dyrektyw unijnych i z niewiążących rekomendacji, oraz uregulowania zaproponowane w projekcie nowego PE, można odnieść wrażenie, że zawarte w projekcie nowego PE regulacje są wierną implementacją rekomendacji KE i grup roboczych. Realizacji tych wytycznych można upatrywać przede wszystkim w powołaniu niezależnego OIP, na którego nałożono obowiązek opracowania obowiązującej wszystkich użytkowników systemu elektroenergetycznego instrukcji informacji pomiarowych, która ma określać m.in. wymagania w zakresie bezpieczeństwa informacji pomiarowych w celu ochrony odbiorców i użytkowników systemu²⁵. Ponadto uwzględniono także inne wytyczne poprzez m.in. określenie z góry podmiotów, którym mogą być przekazywane dane pomiarowe (oraz różnice w tym zakresie w zależności od tego czy mamy do czynienia z danymi indywidualnymi, czy zagregowanymi)²⁶, obowiązek usunięcia danych w braku konieczności dalszego ich przechowywania²⁷, czy też obowiązek sporządzania programu przedsięwzięć służących zapewnieniu ochrony i bezpieczeństwa danych²⁸.

²⁴ Zgodnie z nowym PE jednostkowe dane pomiarowe, w przeciwieństwie do danych zagregowanych, dotyczą danego odbiorcy końcowego (art. 110 ust. 4 nowego PE).

²⁵ Grupa Robocza ds. Ochrony Danych postuluje stworzenie centrum informacyjno-komunikacyjnego, za pośrednictwem którego wszystkie zaangażowane strony uzyskiwałyby dostęp do danych pomiarowych odbiorców oraz opracowanie kodeksu danych pomiarowych obowiązującego wszystkie strony.

²⁶ Zalecenie określenia obowiązków w zakresie bezpieczeństwa i ochrony danych pomiarowych w odniesieniu do wszystkich podmiotów, którym są one udostępniane oraz zalecenie udostępniania określonym podmiotom danych osobowych wyłącznie w zakresie koniecznym do realizacji ich funkcji.

²⁷ Zalecenie określenia maksymalnych okresów archiwizowania danych pomiarowych, po upływie których powinny być one usunięte.

²⁸ Poprzez wprowadzenie tego obowiązku pośrednio spełnione zostało zalecenie wprowadzenia obowiązku określenia systemu oceny skutków w zakresie ochrony danych pomiarowych. Jak się bowiem wydaje, program przedsięwzięć służących zapewnieniu ochrony i bezpieczeństwa danych musi zawierać w sobie także ocenę skutków.

Choć nie wszystkie najważniejsze wytyczne znalazły odzwierciedlenie w projekcie nowego PE²⁹, to jednak szereg istotnych kwestii w nim uregulowano. Reasumując, mimo że projekt nowego PE jest dość ogólny i przewiduje uregulowanie szeregu kwestii szczegółowych w aktach niższej rangi (rozporządzeniu i instrukcji), to wyraźnie i kilkakrotnie podkreślono w nim rangę ochrony danych pomiarowych. W konsekwencji projekt ten stanowi dobry punkt wyjścia do dalszych prac nad uszczegółowieniem systemu ochrony danych pomiarowych. Przerwanie prac nad „dużym trójpakim” spowodowało jednak, że projekt nowego PE nie doczekał się jak dotychczas kolejnej wersji, która zawierałaby bardziej precyzyjne i szczegółowe uregulowania w zakresie ochrony danych pomiarowych. Nie przedstawiono również do tej pory projektu ewentualnego rozporządzenia dotyczącego bezpieczeństwa i ochrony danych pomiarowych, które być może realizowałyby pozostałe unijne zalecenia (choćby takie jak określenie aspektów technicznych ochrony i bezpieczeństwa danych poprzez nakazanie domyślnego ustawienia inteligentnych liczników na ochronę danych pomiarowych czy też stosowania kodowanych kanałów przekazu danych albo doprecyzowanie obowiązków w zakresie ochrony i bezpieczeństwa danych pomiarowych wszystkich podmiotów, którym te dane mają być udostępniane).

2. „Mały trójpak”

Kolejną propozycję w zakresie uregulowania kwestii związanych z wdrożeniem w Polsce systemu inteligentnego opomiarowania zgłoszono w ramach prac nad tzw. małym trójpakim, czyli nowelizacją obecnie obowiązującego PE, mającego na celu implementację unijnych dyrektyw III pakietu liberalizacyjnego i w konsekwencji uniknięcie przez Polskę kar za brak terminowej implementacji³⁰. Pierwszy projekt „małego trójpaku” nie rozwinął jednak koncepcji przyjętej w „dużym trójpaku”. Co więcej, już pierwszy projekt nowelizacji obowiązującego PE, choć w znacznej mierze stanowił powtórzenie regulacji zawartych w „dużym trójpaku”, został pozbawiony niektórych przepisów istotnych z punktu widzenia ochrony danych pomiarowych. Było to zaskakujące, biorąc pod uwagę fakt, że, jak już wspomniano, projekt nowego PE nie realizował wszystkich zaleceń unijnych. Można było zatem oczekiwać, że wraz z postępowaniem prac nad uregulowaniami dotyczącymi wdrożenia w Polsce inteligentnego opomiarowania, kolejne projekty legislacyjne będą zawierać coraz bardziej kompleksową regulację³¹. I tak w projekcie nowelizacji PE zrezygnowano np. z obowiązku usunięcia przez OIP danych pomiarowych w przypadku braku potrzeby dalszego ich archiwizowania oraz obowiązku OIP sporządzania raz na 2 lata, na okres 3 lat, programu przedsięwzięć, jakie należy podjąć w celu zapewnienia bezpieczeństwa i poufności informacji pomiarowych, zawierającego harmonogram przedsięwzięć inwestycyjnych mających na celu utrzymanie standardów niezawodności świadczonych usług, z uwzględnieniem wymaganego poziomu bezpieczeństwa informacji oraz postępu technologicznego. Tym samym usunięto z ustawy jedną z najistotniejszych gwarancji ochrony danych pomiarowych, która stanowiła

²⁹ Przykładowo, nie uwzględniono w dostatecznym stopniu zasady poufności danych z założenia zakładającej domyślne ustawienie liczników na ochronę danych. Nie wprowadzono także wymogu odrębnej zgody odbiorcy dla każdego celu przetwarzania danych pomiarowych. Ponadto nie określono aspektów technicznych zapewnienia bezpieczeństwa danych ani obowiązków w zakresie bezpieczeństwa i ochrony danych pomiarowych w odniesieniu do wszystkich podmiotów, którym są one udostępniane. Nie przewidziano także mechanizmów weryfikacji podmiotów, którym udostępniane są dane pomiarowe, w celu sprawdzenia czy są odpowiednimi i kompetentnymi odbiorcami tych danych.

³⁰ Ustawa z dnia 26 lipca 2013 r. o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Dz.U. z 2013 r. Nr 984).

³¹ Choć „mały trójpak” z założenia miał być aktem przejściowym, regulującym najbardziej palące kwestie do czasu uchwalenia nowego PE, to jednak pierwszy projekt „małego trójpaku” wprowadzał w miarę rozbudowaną regulację w zakresie ochrony i bezpieczeństwa danych pomiarowych bardzo zbliżoną do regulacji zawartej w projekcie nowego PE. Niewielkie zmiany w stosunku do projektu nowego PE trudno wyłumatować przejściowym charakterem „małego trójpaku”.

implementację unijnych zaleceń w tym zakresie. Ponadto, chociaż pozostano przy koncepcji utworzenia niezależnego OIP, zrezygnowano ze szczegółowego określenia w ustawie jego zadań. Oczywiście ustawodawca mógł zakładać, że system ochrony danych pomiarowych zostanie uzupełniony poprzez przepisy wykonawcze oraz instrukcję informacji pomiarowych. Niemniej kwestie najistotniejsze – a usunięte fragmenty dotyczyły kwestii istotnych – powinny znaleźć się w ustawie, a nie aktach niższej rangi. Już zatem na etapie tworzenia pierwszego projektu „małego trójpaku” można było zauważyć złagodzenie reżimu ochrony danych pomiarowych na szczeblu ustawowym.

Ostatecznie jednak w uchwalonym niedawno przez Sejm „małym trójpaku” zrezygnowano z przeważającej części przepisów dotyczących systemu inteligentnego opomiarowania, w tym przepisów dotyczących bezpieczeństwa i ochrony danych pomiarowych. W konsekwencji w zakresie inteligentnego opomiarowania ostatnia nowelizacja PE sprowadziła się do wprowadzenia definicji licznika zdalnego odczytu w nowym art. 9c ust. 5b PE³² oraz do dodania nowego art. 9c ust. 5a PE, zgodnie z którym operatorzy systemów dystrybucyjnych, instalujący u odbiorców końcowych przyłączonych do ich sieci liczniki zdalnego odczytu, są obowiązani chronić dane pomiarowe dotyczące tych odbiorców na zasadach określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych³³. Reasumując, przywołane wyżej przepisy są obecnie jedynymi przepisami w polskim porządku prawnym, które odnoszą się stricte do kwestii danych pomiarowych.

IV. Ocena ostatniej nowelizacji Prawa energetycznego w zakresie ochrony i bezpieczeństwa danych pomiarowych

1. Brak obowiązku instalacji inteligentnych liczników

Pierwsze próby uregulowania kwestii ochrony i bezpieczeństwa danych pomiarowych w kolejnych projektowanych aktach prawnych, tj. projekcie nowego PE oraz nowelizacji obecnego PE potwierdzają, iż w dalszym ciągu nie jest przesądzony ani termin, ani model powszechnego wdrożenia w Polsce systemu inteligentnego opomiarowania. Trzeba bowiem zauważyć, że na przestrzeni 2 lat projekty przeszły zasadniczą ewolucję. Projekt nowego PE zawierał relatywnie kompleksową regulację, przewidującą m.in. obowiązek montażu inteligentnych liczników w określonym czasie i spełniającą niektóre z istotnych wytycznych unijnych w zakresie ochrony danych pomiarowych. Regulacja ta została następnie nieco ograniczona w pierwszym projekcie „małego trójpaku”, aby przyjąć wręcz zdawkową postać w ostatecznie uchwalonej ostatniej nowelizacji PE. W tym kontekście warto odpowiedzieć na pytanie: czy zaproponowane obecnie zmiany w PE były potrzebne i czy są wystarczające, a w konsekwencji, czy niezbędne są bardziej szczegółowe uregulowania w zakresie ochrony i bezpieczeństwa danych pomiarowych.

W pierwszej kolejności warto zwrócić uwagę, że w uchwalonej nowelizacji PE ostatecznie nie wprowadzono obowiązku montażu liczników inteligentnych w z góry określonym czasie (pomimo

³² Przez licznik zdalnego odczytu rozumie się zespół urządzeń służących do pozyskiwania danych pomiarowych, umożliwiający dwustronną komunikację z systemem teleinformatycznym. Licznik zdalnego odczytu jest odpowiednikiem licznika inteligentnego, o którym była mowa w projekcie nowego PE. W konsekwencji wszelkie odniesienia w artykule do licznika inteligentnego dotyczą także licznika zdalnego odczytu.

³³ Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm. (ustawa o ochronie danych osobowych).

iz taka regulacja była w pierwotnym projekcie „małego trójpaku”). Pomijając że, jak wskazano wcześniej, Polska tym samym nie wdrożyła dyrektywy 2009/72/WE przewidującej montaż liczników inteligentnych u 80% odbiorców do 2020 r.³⁴, fakt ten ma istotne znaczenie także w kontekście wynikających z regulacji unijnych oraz Konstytucji RP gwarancji ochrony danych osobowych (które należy odnosić także do danych pomiarowych) w zestawieniu z celami wdrożenia inteligentnego opomiarowania.

Zgodnie z art. 8 Karty praw podstawowych UE dane osobowe mogą być przetwarzane za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Niezależnie od tego zgodnie z art. 51 ust. 1 Konstytucji nikt nie może być zobowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby. W konsekwencji, o ile odbiorca nie wyrazi zgody na pozyskiwanie i przetwarzanie jego danych osobowych, w braku przepisów rangi ustawowej zobowiązujących go do tego, dane takie nie mogą być pozyskiwane ani przetwarzane (zasadę tę należy odnosić także do danych pomiarowych). Jednakże, jak wskazano wcześniej, odbiorcy energii elektrycznej zaniepokojeni potencjalnym naruszeniem ich prawa do prywatności w związku z montażem liczników inteligentnych mogą gremialnie nie wyrażać zgody na przetwarzanie ich danych pomiarowych³⁵. Może to doprowadzić do skutku w postaci nieosiągnięcia jednego z zakładanych celów wdrożenia inteligentnego opomiarowania, a mianowicie obniżenia zużycia energii w skali makro³⁶. A zatem, aby powyższy skutek został osiągnięty, uprawnienie do pozyskiwania i przetwarzania danych pomiarowych z liczników inteligentnych powinno wynikać z przepisów prawa rangi ustawowej, tak aby na montaż liczników inteligentnych nie była potrzebna zgoda odbiorców³⁷. Mając powyższe na uwadze, trzeba wskazać, że ostatnia nowelizacja PE takiej podstawy nie przewidziała, w przeciwieństwie do wcześniejszych propozycji ustawowych³⁸. W konsekwencji w obecnym stanie prawnym istnieje konieczność każdorazowego uzyskania zgody odbiorcy na montaż licznika inteligentnego, ponieważ ten ze swej natury rejestruje i przekazuje dokładne dane pomiarowe pozwalające choćby w pośredni sposób na identyfikację danego odbiorcy. Oczywiście nie można z góry założyć, że odbiorcy powszechnie nie będą wyrażać zgody na montaż liczników inteligentnych. Biorąc jednak pod uwagę doświadczenia w innych krajach, wydaje się, że bezpieczniejszym rozwiązaniem, zapewniającym osiągnięcie celu powszechnego wdrożenia inteligentnego opomiarowania, jest ustawowe wprowadzenie obowiązku ich montażu. Niezależnie od tego wprowadzenie takiego obowiązku stanowiłoby, jak wspomniano, konieczną implementację dyrektywy 2009/72/WE.

³⁴ Vide przypis nr 3. Trudno uznać za wypełnienie tego zobowiązania nałożenie na operatorów zgodnie z art. 16 ust. 7 pkt 4 PE obowiązku uwzględnienia w planach rozwoju w zakresie zaspokojenia obecnego i przyszłego zapotrzebowania na paliwa gazowe lub energię przedsięwzięć racjonalizujących zużycie paliw lub energii u odbiorców, w tym także przedsięwzięć w zakresie pozyskiwania, transmisji oraz przetwarzania danych pomiarowych z licznika zdalnego odczytu. Niezrealizowanie tego obowiązku jest o tyle zaskakujące, że ostatnia nowelizacja PE miała na celu wdrożenia m.in. dyrektywy 2009/72/WE i w konsekwencji zapobieżenia nałożeniu na Polskę kar pieniężnych za brak terminowej implementacji.

³⁵ W Europie taka sytuacja miała miejsce w Holandii, gdzie brak zapewnienia odpowiedniego poziomu ochrony i bezpieczeństwa danych pomiarowych przy pierwszych próbach wdrożenia systemu inteligentnego opomiarowania spowodował tak silny opór społeczny, że ostatecznie przyjęto tam model pozwalający odbiorcom na odmowę instalacji inteligentnego licznika; zob. R. Knyrim, G. Trieb, *Smart metering under...*, s 122).

³⁶ Vide przypis nr 9.

³⁷ Choć z punktu widzenia ochrony prawa do prywatności można mieć pewne wątpliwości co do wprowadzenia takiego obowiązku, to jednak trzeba mieć na uwadze cel wprowadzenia systemu inteligentnego opomiarowania. W mojej opinii cel ten usprawiedliwia taki obowiązek, przy założeniu jednak, że na poziomie ustawowym zostanie zapewniony odpowiedni poziom ochrony i bezpieczeństwa danych pomiarowych odbiorców. Zob. R. Knyrim, G. Trieb, *Smart metering under...*, s 126).

³⁸ Przewidziany w „dużym trójpaku” i pierwszym projekcie „małego trójpaku” obowiązek montażu inteligentnych liczników u odbiorców bez przewidzenia prawa sprzeciwu odbiorcy w połączeniu z uregulowaniem zasad pozyskiwania i udostępnienia danych pomiarowych (indywidualnych i zagregowanych) można uznać za podstawę ustawową do przetwarzania danych pomiarowych.

2. Obowiązek ochrony danych pomiarowych zgodnie z przepisami ustawy o ochronie danych osobowych

W mojej ocenie warto także odpowiedzieć na pytanie: czy wprowadzenie ostatnią nowelizacją PE obowiązku ochrony danych pomiarowych na zasadach określonych w ustawie o ochronie danych osobowych było w ogóle potrzebne. Jak bowiem wspomniano wcześniej, na obecnym etapie nie podjęto jeszcze decyzji o powszechnym wdrożeniu w Polsce systemu inteligentnego opomiarowania poprzez ustanowienie obowiązku montażu inteligentnych liczników. Czy zatem w tym kontekście w ogóle potrzebne jest regulowanie w jakikolwiek szczególny sposób kwestii ochrony danych pomiarowych? Odpowiedź na to pytanie nie jest jednoznaczna.

Z jednej strony bowiem przepisy znowelizowanego PE nałożyły na operatorów pewne miękkie obowiązki w zakresie wdrażania inteligentnego opomiarowania poprzez określenie w art. 16 ust. 7 pkt 4 PE, że plan rozwoju w zakresie zaspokojenia obecnego i przyszłego zapotrzebowania na paliwa gazowe lub energię powinien zawierać m.in. przedsięwzięcia racjonalizujące zużycie paliw i energii u odbiorców, w tym także przedsięwzięcia w zakresie pozyskiwania, transmisji oraz przetwarzania danych pomiarowych z licznika zdalnego odczytu. Ustawodawca zatem nałożył pośrednio na operatorów obowiązek przynajmniej planowania przedsięwzięć w zakresie instalacji inteligentnych liczników i przetwarzania danych w nich gromadzonych. Można zatem zakładać, że skutkiem tego rodzaju planowania będzie montaż inteligentnych liczników u coraz większej liczby odbiorców. Zresztą już obecnie pewne pilotażowe projekty dotyczące inteligentnego opomiarowania u odbiorców końcowych są realizowane, a kolejne wkrótce się rozpoczną. Najstarszy i najbardziej rozbudowany z takich projektów prowadzi obecnie Energa Operator SA³⁹. Podobne plany ma także RWE Stoen Operator sp. z o.o., który ogłosił już przetarg na doradztwo przy wdrażaniu systemu inteligentnego opomiarowania⁴⁰. Również inni operatorzy prowadzą programy pilotażowe inteligentnego opomiarowania. Mając powyższe na uwadze, należałoby pozytywnie ocenić wprowadzenie w ostatniej nowelizacji PE uregulowania, które – choć zdawkowo – to jednak bezpośrednio odnosi się do ochrony danych pomiarowych. Nie dość bowiem, że w praktyce już obecnie te dane są gromadzone i przetwarzane w ramach programów pilotażowych, to w najbliższej przyszłości można spodziewać się coraz większej liczby takich projektów realizowanych na coraz szerszą skalę. Konsekwencją powyższego powinno być zatem objęcie danych pomiarowych odpowiednią ochroną.

Z drugiej strony, można mieć wątpliwości czy ustawodawca słusznie postąpił, ograniczając całą regulację w zakresie ochrony danych pomiarowych do jednego przepisu (art. 9c ust. 5a PE) po prostu odsyłającego do przepisów ustawy o ochronie danych osobowych i nie wprowadzając żadnych dodatkowych gwarancji ochrony danych pomiarowych. W praktyce bowiem jedynie potwierdzono na poziomie ustawowym, że dane pomiarowe podlegają takiej samej ochronie jak dane osobowe. Trzeba jednak przypomnieć, jak wskazano wcześniej, iż od początku rozważań nad kwestią ochrony danych pomiarowych nigdy nie kwestionowano, że dane pomiarowe mogą stanowić dane osobowe. Wręcz przeciwnie, konsekwentnie przypomniano, że dane

³⁹ Zgodnie z informacją na stronie internetowej Energa Operator S.A., aktualnie we wszystkich gospodarstwach domowych w Kaliszu zainstalowane są inteligentne liczniki. Od wiosny 2013 r. przy udziale około 1700 mieszkańców Kalisza organizowany jest test konsumencki systemów inteligentnego opomiarowania.

⁴⁰ Przetarg nr FZ-Z/P062/13 na świadczenie doradczych usług prawnych w zakresie Prawa Zamówień Publicznych na potrzeby Projektu AMI (Zaawansowanej Infrastruktury Pomiarowej).

miarowe podlegają co najmniej takiej samej ochronie, jak dane osobowe i dodatkowo podkreślano konieczność ustanowienia dalej idącej ochrony ze względu na szczególną specyfikę danych pomiarowych i szczególne zagrożenia wiążące się z ich nieuprawnionym wykorzystaniem. Konsekwencją powyższego jest, że do danych pomiarowych miały i mają zastosowanie nie tylko unijne,⁴¹ lecz także polskie przepisy o ochronie danych osobowych, które przecież unijne przepisy implementują. Zgodnie zresztą z art. 6 ust. 1 ustawy o ochronie danych osobowych, za dane osobowe uważa się wszelkie informacje dotyczące nie tylko zidentyfikowanej, ale także możliwej do zidentyfikowania osoby fizycznej. Nie ma natomiast wątpliwości, że dane o zużyciu energii w określonym punkcie pomiarowym w połączeniu z innymi informacjami, np. na temat osoby, która jest stroną umowy z przedsiębiorstwem energetycznym dotyczącej tego punktu, pozwalają na choćby pośrednie zidentyfikowanie danego odbiorcy energii lub grupy odbiorców⁴². Zgodnie z kolei z art. 1 ust. 1 ustawy o ochronie danych osobowych, każdy ma prawo do ochrony dotyczących go danych osobowych. W konsekwencji, w mojej ocenie, nawet przed ostatnią nowelizacją PE dane pomiarowe podlegały ochronie na podstawie ustawy o ochronie danych osobowych i nie było w związku z tym potrzeby przesądzania o tym w PE. Mogłoby się jednak wydawać, iż potwierdzenie na poziomie ustawowym oczywistego faktu, zgodnie z którym dane pomiarowe podlegają takiej samej ochronie, jak dane osobowe, było dobrym posunięciem. Wszak można byłoby twierdzić, że w ten sposób ustawodawca podkreślił istotę ochrony danych pomiarowych. Nie było to jednak najlepsze posunięcie, biorąc pod uwagę zasady prawidłowej legislacji. Stosując bowiem wykładnię *a contrario*, można dojść do wniosku, że inne dane specjalistyczne, nawet jeżeli wypełniają definicję danych osobowych z ustawy o ochronie danych osobowych, nie podlegają ochronie na podstawie tej ustawy, jeżeli nie przesądzono o tym wyraźnie w ustawie specjalnej odnoszącej się do tych specjalistycznych danych. Odnosząc powyższe rozważania konkretnie do ochrony danych pomiarowych, trzeba przypomnieć, jak wskazano wcześniej, iż bezspornie do ochrony danych pomiarowych stosuje się postanowienia nie tylko dyrektywy 95/46/WE, lecz także dyrektywy 2002/58/WE. Ustawa o ochronie danych osobowych implementuje jednak tylko dyrektywę 95/46/WE. Dyrektywa 2002/58/WE została natomiast implementowana przepisami ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne⁴³. Oczywiste jest zatem, że już obecnie do ochrony danych pomiarowych należałoby stosować także przepisy prawa telekomunikacyjnego w zakresie dotyczącym transmisji danych pomiarowych, skoro stanowią implementację dyrektywy 2002/58/WE. Niemniej ostatnia nowelizacja PE odsyła wyraźnie tylko do przepisów ustawy o ochronie danych osobowych, w odniesieniu natomiast do transmisji danych nie przewiduje odpowiedniego stosowania przepisów prawa telekomunikacyjnego. A zatem, choć taka wykładania byłaby kuriozalna, można byłoby dojść do wniosku, że *a contrario* do ochrony danych pomiarowych (w zakresie transmisji danych pomiarowych) nie stosuje się przepisów prawa telekomunikacyjnego.

⁴¹ Jednoznacznie potwierdzono to w pkt. 7 preambuły Zaleceń KE.

⁴² Jak wskazano wcześniej, danego odbiorcy energii można zidentyfikować choćby w pośredni sposób, nawet jeżeli nie jest stroną umowy z przedsiębiorstwem energetycznym. Niezależnie od tego, jak się wydaje, można przyjąć, że dane pomiarowe z danego licznika będą danymi osobowymi przynajmniej osoby będącej stroną umowy z przedsiębiorstwem energetycznym. Dane o zużyciu energii w danym punkcie pomiarowym, którego dotyczy określona umowa, zawsze przecież będą mogły być przypisane osobie, która podpisała umowę, nawet jeżeli faktycznie w lokalu przebywała większa liczba osób lub nawet ktoś inny. Jak się wydaje, z punktu widzenia prawa do prywatności danej osoby pozostaje bez znaczenia czy określone dane pomiarowe dotyczą tylko tej osoby, skoro faktycznie mogą być jej przypisane. Dlatego jak się wydaje można przyjąć, że dane pomiarowe z określonego punktu pomiarowego stanowią dane osobowe osoby będącej stroną umowy dotyczącej tego punktu.

⁴³ Dz.U. z 2004 r. Nr 171, poz. 1800 z późn. zm. (dalej: PK).

Reasumując, w mojej ocenie wprowadzenie do PE regulacji po prostu odsyłającej do przepisów ustawy o ochronie danych osobowych nie było dobrym posunięciem. Skoro ustawodawca na tym etapie nie zdecydował się na kompleksowe uregulowanie w PE kwestii ochrony i bezpieczeństwa danych pomiarowych (pomimo iż pewne projekty w tym zakresie są już realizowane i dane pomiarowe są w praktyce gromadzone i przetwarzane), to nie powinien w ogóle wprowadzać jakichkolwiek przepisów w tym zakresie. Jak bowiem wskazano, wprowadzenie odesłania do przepisów ustawy o ochronie danych osobowych w praktyce nic nie zmienia, a może powodować niepotrzebne trudności interpretacyjne i na pewno nie stanowi przykładu dobrej praktyki legislacyjnej. Ponadto negatywnie oceniam fakt, iż skoro ustawodawca dostrzegł konieczność zapewnienia ochrony danych pomiarowych już na obecnym etapie (inaczej bowiem nie wprowadziłby żadnych przepisów w tym zakresie), to nie zrobił tego w sposób realizujący chociaż część wskazanych wcześniej unijnych zaleceń. Nawet bowiem bez wprowadzania jeszcze na tym etapie obowiązku montażu liczników inteligentnych, można było przyjąć w ostatniej nowelizacji część dobrych rozwiązań w zakresie ochrony i bezpieczeństwa danych osobowych zaproponowanych w projekcie nowego PE. Wydaje się, że właśnie w fazie realizacji programów pilotażowych zapewnienie odpowiedniego poziomu bezpieczeństwa jest najistotniejsze. Ewentualne naruszenia w tym zakresie mogą bowiem zaważyć na przyszłości systemu inteligentnego opomiarowania w Polsce.

V. Potrzeba nowelizacji polskich przepisów prawa w zakresie ochrony i bezpieczeństwa danych pomiarowych

1. Czy przepisy ustawy o ochronie danych osobowych są wystarczające?

Skoro jednak w przepisach PE wyraźnie przesądzono, że dane pomiarowe podlegają ochronie na podstawie ustawy o ochronie danych osobowych, to należałoby także odpowiedzieć na pytanie, czy w ogóle potrzebne są dalsze zmiany w prawie. Teoretycznie można przecież argumentować, że polski ustawodawca uchwalając ustawę o ochronie danych osobowych, miał na celu jak najlepszą ochronę danych osobowych, przy odpowiednim wyważeniu interesów podmiotów zainteresowanych pozyskiwaniem i przetwarzaniem tych danych. Skoro tak, to dane pomiarowe z liczników inteligentnych, które przecież, jak wskazano, można traktować jak dane osobowe, powinny być w dostateczny sposób chronione. W przeciwnym razie można byłoby dojść do wniosku, iż przepisy ustawy o ochronie danych osobowych nie zapewniają dostatecznej ochrony co do zasady (skoro nie chronią w dostateczny sposób danych pomiarowych, które można traktować jak dane osobowe). Przesądzenie powyższej kwestii nie jest jednak wcale jednoznaczne. Trzeba bowiem wskazać, iż ustawa o ochronie danych osobowych jest aktem o bardzo ogólnym charakterze. Poniekąd jest to zrozumiałe, skoro ma znaleźć zastosowanie do wielu różnych rodzajów danych. Określony dla danego typu danych osobowych stopień ochrony mógłby być zbyt rygorystyczny dla innego rodzaju danych. Dlatego, jak się wydaje, nie można *a priori* zakładać, iż objęcie danych pomiarowych ochroną na podstawie przepisów ustawy o ochronie danych osobowych jest wystarczające. Potwierdza to także treść art. 5 ustawy o ochronie danych osobowych, zgodnie z którym jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z tej ustawy, stosuje się przepisy tych ustaw. A zatem można wywodzić, iż ustawodawca brał pod uwagę sytuacje, w których określony typ danych będzie

wymagał ustanowienia w przepisach szczególnych dalej idącej ochrony niż wynikająca z przepisów ustawy o ochronie danych osobowych. W związku z tym samo objęcie danych pomiarowych ochroną na zasadach określonych w ustawie o ochronie danych osobowych nie musi przesądzać, że taka ochrona jest wystarczająca.

W powyższym kontekście warto zatem krótko przeanalizować, czy przepisy ustawy o ochronie danych osobowych mimo wszystko nie są wystarczające, biorąc pod uwagę wskazane wcześniej wymogi ochrony danych pomiarowych wynikające z dyrektyw i niewiążących zaleceń unijnych. Po pierwsze, zgodnie z art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych przetwarzanie danych osobowych jest dopuszczalne wtedy, m.in. gdy osoba, której dane dotyczą, wyrazi na to zgodę⁴⁴. Zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych administrator danych osobowych jest obowiązany poinformować tę osobę m.in. o celu zbierania danych, prawie dostępu do danych osobowych i ich poprawiania. Ponadto administrator, zgodnie z art. 26 ust. 1 ustawy o ochronie danych osobowych, jest obowiązany zapewnić, aby dane były m.in. zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Co więcej, zgodnie z art. 32 ust. 1 ustawy o ochronie danych osobowych, każdej osobie przysługuje prawo do kontroli przetwarzania jej danych osobowych zawartych w zbiorach danych, w tym m.in. prawo do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane. Wreszcie trzeba wskazać, że zgodnie z art. 36 ustawy o ochronie danych osobowych, administrator jest obowiązany stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zebraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Mając na uwadze powyższe najważniejsze gwarancje wynikające z ustawy o ochronie danych osobowych trzeba stwierdzić, że są one zbieżne z wymogami wynikającymi z dyrektywy 95/46/WE, które wskazano wcześniej. Jest to naturalne, biorąc pod uwagę, że polskie przepisy implementują tę dyrektywę. Polskie przepisy nie idą jednak w ochronie danych dalej, niżby to z tych dyrektyw wynikało.

2. Spodziewane zmiany w systemie ochrony danych osobowych na poziomie unijnym

W kontekście rozważań nad koniecznością bardziej szczegółowego uregulowania w Polsce kwestii ochrony i bezpieczeństwa danych pomiarowych, należy jednak w mojej ocenie wziąć pod

⁴⁴ Art. 23 ust. 1 wskazuje także inne podstawy przetwarzania danych, jednak pozostają one nierelwantne w kontekście danych pomiarowych. W braku przepisów szczególnych nakładających obowiązek instalacji liczników inteligentnych i wskazujących cele, jakim ma to służyć, w praktyce obecnie wyłącznie zgoda odbiorcy daje prawo do przetwarzania danych pomiarowych. Na marginesie trzeba wskazać, iż przesłanka w postaci konieczności realizacji umowy nie znajduje zastosowania, ponieważ w celu dokonania rozliczeń zużycia energii nie jest konieczne posykanie tak szczegółowych danych, jakie w założeniu mają dostarczać liczniki inteligentne. Istota inteligentnego licznika polega bowiem na tym, że przekazywane przez niego dane są dość szczegółowe, aby z jednej strony pozwolić operatorom na optymalne sterowanie systemem, a z drugiej zaś – umożliwić odbiorcom skuteczne sterowanie swoim zużyciem. Obecnie zakłada się, że liczniki inteligentne będą przekazywały dane co 15 minut (*vide* przypis nr 51). Ponadto, jak słusznie twierdzi Tomasz Kowalak, regulator nie będzie raczej akceptował kosztów wymiany liczników indukcyjnych na takie, które pozwolą wyłącznie na realizację funkcji bilingu, gdyż działanie takie byłoby klasycznym przykładem ewidentnego zawężania możliwych funkcjonalności, szkodliwego dla osiągnięcia zakładanych celów montażu inteligentnych liczników. Zob. T. Kowalak, *Smart Grid – Wyzwanie XXI Wieku*, „Rynek Energii” 2010, nr 6(V), s. 80.

uwagę także projektowane nowe przepisy unijne dotyczące ochrony danych osobowych. Istota tych zmian polega bowiem na zastąpieniu aktualnej dyrektywy 95/46/WE rozporządzeniem określającym ogólne unijne ramy ochrony danych⁴⁵. A zatem przyszłe rozporządzenie unijne o ochronie danych pomiarowych będzie stosowane w Polsce wprost bez konieczności jego implementacji. Jeżeli zatem przyszłe rozporządzenie będzie zapewniać dalej idącą ochronę danych osobowych niż dyrektywa 95/46/WE i realizować chociaż część zaleceń unijnych odnoszących się do danych pomiarowych, to odpowiednio w mniejszym zakresie będą potrzebne zmiany w polskim prawie.

Projekt nowego rozporządzenia został przedstawiony przez KE 25 stycznia 2012 r.⁴⁶. Przede wszystkim jego założeniem jest ujednoczenie przepisów dotyczących ochrony danych osobowych w UE oraz dostosowanie zasad ochrony danych do postępu technologicznego i globalizacji „w celu wzmocnienia prawa do prywatności w internecie i nadania impulsu gospodarce cyfrowej”⁴⁷. Niemniej pewne kwestie uregulowano w rozporządzeniu bardziej szczegółowo niż w dotychczasowej dyrektywie 95/46/WE. Z niewiążących zaleceń unijnych w projekcie rozporządzenia uwzględniono jednak tylko dwa zalecenia. Po pierwsze, zgodnie z art. 23 projektu rozporządzenia zwrócono uwagę na konieczność uwzględniania ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej (choć uregulowano to w dość ogólny sposób), natomiast w art. 33 przewidziano obowiązek przeprowadzania przez administratorów i podmioty przetwarzające oceny skutków w zakresie ochrony danych przed podjęciem ryzykownych operacji ich przetwarzania. A zatem, jeżeli brać za punkt odniesienia niewiążące wytyczne unijne w zakresie ochrony i bezpieczeństwa danych pomiarowych, to konieczne będą zmiany w polskich przepisach prawa pomimo wejścia w życie nowego rozporządzenia unijnego w zakresie ochrony i bezpieczeństwa danych pomiarowych⁴⁸.

3. Potrzeba zmian w polskim prawie

Tak jak wskazano powyżej, ostatnia nowelizacja PE nie spowodowała zapewnienia lepszej ochrony danych pomiarowych niż już wynikająca z obowiązujących przepisów o ochronie danych osobowych, które w istocie odpowiadają wymogom unijnych dyrektyw w tym zakresie. Trzeba jednak przypomnieć, iż pomimo systemu ochrony wynikającego z dyrektyw, KE i inne niezależne podmioty europejskie stworzyły szereg dalej idących wytycznych. A zatem podmioty te uznały, że ochrona wynikająca z dyrektyw nie jest wystarczająca w odniesieniu do danych pomiarowych. Jak wskazano, ostatnie zmiany PE nie realizują tych zaleceń. Z kolei projekt nowego unijnego rozporządzenia o ochronie danych osobowych realizuje tylko niektóre z nich. Choć zalecenia unijne nie są wiążące, to jednak wyznaczają pewien pożądany w UE standard ochrony danych pomiarowych, nie negując przy tym potrzeby powszechnego wdrożenia systemów inteligentnego opomiarowania w całej UE. Można zatem przyjąć, iż wytyczne te nie są zbyt daleko idące. W konsekwencji jestem zdania, iż wytyczne te powinny zostać uwzględnione przez polskiego ustawodawcę. Warto zatem zastanowić się, w jakim kierunku powinny pójść przyszłe zmiany w prawie, aby w Polsce

⁴⁵ Komunikat prasowy KE z 25.01.2012 r., IP/12/46.

⁴⁶ Wniosek KE COM(2012) 11, Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych).

⁴⁷ Komunikat prasowy KE z 25.01.2012 r., IP/12/46.

⁴⁸ Przy założeniu, że nowe rozporządzenie wejdzie w życie w takiej formie, jak obecny projekt. Zgodnie z zapowiedziami KE, nowe rozporządzenie ma wejść w życie dopiero w 2014 r., a zatem do tego czasu obecny, pierwszy projekt może ulec daleko idącym zmianom.

osiągnięty został standard ochrony i bezpieczeństwa danych pomiarowych określony unijnymi wytycznymi.

Po pierwsze jestem zdania, iż nie powinno się dokonywać kolejnej nowelizacji aktualnego PE. Ponieważ rząd zadeklarował zamiar kontynuowania prac nad nowym PE, to w nim i aktach wykonawczych do niego powinny znaleźć się przepisy wdrażające zalecenia unijne. Niemniej najistotniejsze kwestie powinny znaleźć się w samej ustawie, a nie w rozporządzeniu (a tym bardziej w instrukcji informacji pomiarowych). Stanowiłoby to zresztą kontynuację dotychczasowych prac nad nowym PE, którego projekt, jak wskazano, już teraz realizuje szereg istotnych wytycznych unijnych i w konsekwencji stanowi dobry punkt wyjścia do dalszych prac nad uszczegółowieniem systemu ochrony i bezpieczeństwa danych pomiarowych. W konsekwencji uważam, że rozwiązania zaproponowane w projekcie nowego PE powinny pozostać w ostatecznej wersji ustawy. Pozytywnie oceniam między innymi określenie z góry podmiotów, którym dane będą udostępniane z uwzględnianiem różnic pomiędzy danymi zagregowanymi i indywidualnymi, obowiązek przygotowywania przez OIP analizy w zakresie rodzajów ryzyka i środków zaradczych w zakresie ochrony i bezpieczeństwa danych pomiarowych. Dodatkowo postanowienia te powinny zostać uzupełnione o bardziej szczegółowe uregulowania na poziomie samej ustawy. Przykładowo w projekcie nowego PE nie ma mowy o ochronie danych już w fazie projektowania⁴⁹. Zgodnie natomiast z Zaleceniami KE, ochrona danych w fazie projektowania powinna być wdrażana na poziomie ustaw⁵⁰ (a nie w aktach niższej rangi). A zatem w nowym PE powinny znaleźć się wymogi w tym zakresie. Teoretycznie można byłoby rozważyć, czy istnieje potrzeba uregulowania tej kwestii w nowym PE, skoro jak wspomniano, ma być to uregulowane w nowych unijnym rozporządzeniu o ochronie danych osobowych (skoro rozporządzenie będzie obowiązywać wprost, to nie powinno się polską ustawą regulować tych samych kwestii). Z jednej strony, ostateczny kształt ani moment wejścia w życie tego rozporządzenia nie są jednak jeszcze znane, a więc do czasu jego uchwalenia może zająć potrzeba uregulowania kwestii ochrony i bezpieczeństwa danych pomiarowych. Z drugiej zaś – rozporządzenie zawiera jedynie bardzo ogólne postanowienia w tym zakresie. Podobnie ogólnie w projekcie rozporządzenia ujęto wymóg zapewniania domyślnej ochrony danych. Zgodnie z kolei z opinią Grupy Roboczej ds. Ochrony Danych na najbardziej podstawowym poziomie koncepcja „prywatności z założenia” zapewnia przesyłanie odczytów licznika wyłącznie z taką częstotliwością, jaka jest konieczna dla funkcjonowania systemu lub świadczenia usługi, na jaką zgodził się klient⁵¹. Nowe rozporządzenie unijne o ochronie danych osobowych, pomimo iż porusza w art. 23 kwestię ochrony danych jako opcji domyślnej, to nie określa częstotliwości pobierania danych. Określenie częstotliwości zbierania danych pomiarowych jest zresztą jedną z najistotniejszych kwestii w kontekście poszanowania prawa do prywatności odbiorców. Im bowiem częstsze odczyty, tym dokładniej można odtworzyć cykl życiowy danej osoby i tym bardziej narusza się jej prywatność. A zatem kwestia częstotliwości zbierania danych powinna być uregulowana w samej ustawie, a nie przykładowo w rozporządzeniu, co przewiduje obecny projekt nowego PE. Podzielam przy tym zdanie większości uczestników rynku, że częstotliwość

⁴⁹ Zgodnie z pkt I ust. 3 lit. d) Zaleceń KE „Ochrona danych już w fazie projektowania” wymaga wdrożenia, z uwzględnieniem najnowszych osiągnięć technicznych oraz kosztów wdrożenia zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, odpowiednich środków i procedur technicznych i organizacyjnych, tak aby przetwarzanie odpowiadało wymogom dyrektywy 95/46/WE oraz gwarantowało ochronę praw osoby, której dotyczą dane.

⁵⁰ Pkt I ust. 12 Zaleceń KE.

⁵¹ Opinia Grupy roboczej ds. Ochrony Danych, s. 10.

zbierania danych pomiarowych powinna być nie większa niż co 15 minut⁵². Uważam także, że nowe PE na poziomie ustawowym powinno określać, zgodnie z zaleceniami unijnymi, maksymalny okres archiwizowania danych pomiarowych, po upływie którego dane powinny zostać usunięte.

VI. Zakończenie

Ochrona danych pomiarowych jest jednym z najistotniejszych elementów wdrażania systemów inteligentnego opomiarowania. Niezapewnienie odpowiedniej ochrony może spowodować, iż powszechne wdrożenie takiego systemu w Polsce się nie powiedzie. Pomimo tego polski ustawodawca nie zdecydował się na zapewnienie ochrony danych pomiarowych dalej idącej niż ochrona wynikająca z ogólnych unijnych i polskich przepisów o ochronie danych osobowych. W tym kontekście uznaję za konieczne dokonanie zmian w polskim prawie zmierzających do realizacji niewiążących zaleceń unijnym w zakresie ochrony i bezpieczeństwa danych pomiarowych. Na obecnym etapie, kiedy przetwarzanie danych pomiarowych odbywa się wyłącznie na podstawie zgody odbiorcy, zapewnienie dalej idącej ochrony niż wynikająca z dyrektyw unijnych nie jest absolutnie niezbędne⁵³. Jednak w przyszłości, zwłaszcza gdyby montaż liczników inteligentnych był obowiązkowy, konieczne będzie w mojej ocenie wdrożenie Zaleceń KE i innych unijnych rekomendacji i to na poziomie ustawowym. Skoro bowiem na szczeblu unijnym uznano, że dane pomiarowe powinny być lepiej chronione niż to wynika w ogólnych przepisów o ochronie danych osobowych, to wydaje się, że nie ma racjonalnych powodów, aby w Polsce ten model ochrony danych pomiarowych nie był implementowany. Zgodnie z deklaracjami rządu, prace nad „dużym trójpakietem” będą kontynuowane. Można zatem mieć nadzieję, że przepisy w zakresie ochrony i bezpieczeństwa danych pomiarowych zaproponowane w projekcie nowego PE zostaną poprawione i odpowiednio uzupełnione. Projekt ten realizuje bowiem część istotnych zaleceń unijnych i stanowi tym samym dobry punkt wyjścia do dalszych prac. Oczywiście nie wszystkie kwestie wymagają uregulowania na poziomie ustawowym. W pewnym zakresie doprecyzowania zasad ochrony i bezpieczeństwa danych pomiarowych można dokonać w przyszłym rozporządzeniu i instrukcji informacji pomiarowych. Nowe PE powinno jednak zawierać w tym zakresie jasne wytyczne, a nie jedynie blankietowo wskazywać na konieczność wzięcia pod uwagę aspektu bezpieczeństwa i ochrony danych pomiarowych przy tworzeniu tych dokumentów.

⁵² Jak się wskazuje z jednej strony dane 15-minutowe są wystarczające do zapewnienia funkcjonalności inteligentnych liczników, z drugiej zaś – częstsze zbieranie danych stanowiłoby zbyt daleko idącą ingerencję w prywatność odbiorców, nieuzasadnioną celami, dla których te dane są zbierane. Stanowisko to podziela m.in. Główny Inspektor Danych Osobowych (wywiad z 21.11.2014 r. dla wp.pl pt. *GIODO: inteligentne opomiarowanie to wyzwanie dla energetyki*, dostępny na stronie internetowej GIOGO pod adresem http://www.giodo.gov.pl/plik/id_p/3496/j/pl/). Podobnie: J. Zimmer-Czekaj, *Przetwarzanie danych pomiarowych przez OSD*, „Energia elektryczna”, 2013, czerwiec, s. 12.

⁵³ Zakładając, że operatorzy sieci prawidłowo stosują przepisy ustawy o ochronie danych osobowych, można przyjąć, że przed udzieleniem zgody odbiorcy są dokładnie informowani o celu i zakresie przetwarzania ich danych pomiarowych, a ich zgoda jest wyraźna i w pełni świadoma. Skoro zatem bez świadomej zgody odbiorcy nie można obecnie przetwarzać jego danych osobowych, a nawet, jak się wydaje, zamontować mu inteligentnego licznika, to dalej idąca ochrona niż wynikająca z aktualnie obowiązujących przepisów nie jest absolutnie niezbędna.